Data protection in health and telematics projects compliance with legal and ethical requirements

Louveaux, Sophie; Poullet, Yves

Published in:
Computer Law and Security Report

Publication date:
1996

Document Version
Publisher's PDF, also known as Version of record

DATA PROTECTION IN HEALTH AND TELEMATICS PROJECTS COMPLIANCE WITH LEGAL AND ETHICAL REQUIREMENTS[1]

Sophie Louveaux and Yves Poullet consider the impact of the recent EC Data Protection Directive on the protection of personal data in computerized healthcare systems. Particular attention is paid to the problem of improving transparency within the network.

INTRODUCTION

The use of telematics in the healthcare sector will modify the existing pattern of relationships between healthcare professionals and their patients. Traditionally any personal information was collected from the patient himself and registered on a paper-based system. Any exchange of personal data between healthcare professionals was therefore limited by practical constraints and very often did not go beyond the institutional framework (hospital, clinic,...). The rules governing professional secrecy were considered adequate in order to exercise control over the exchanges of personal medical information.

Telematics introduces the use of networks, increasing the number of players involved in the exchanges of information and thereby extends the initial bilateral relationship between a healthcare professional and his patient. The rules governing professional secrecy will no longer be considered as sufficient in order to guarantee the patient's right to privacy and confidentiality of his medical data. Adequate rules governing the exchanges of information must be enacted so as to ensure that the medical data is only transmitted to authorized users for specific and legitimate purposes and not further used by these users for other secondary purposes. Measures must be taken in order to define and control the flows of information: Who may receive the data? For what reasons? And under what conditions (drawing up of adequate security measures, transparency of the exchanges with regard to the data subject...)?

A number of different international and national legal instruments will apply in order to afford data protection in telematics. Notably one can mention:

- OECD Guidelines governing the protection of privacy and transborder flows of personal data; 23 September 1980
- Council of Europe Convention No.108 for the protection of individuals with regard to automatic processing of personal data, 28 January 1981
- Council of Europe Recommendation No. (81)1 for automated medical data banks, 23 January 1981 (currently under review: Council of Europe draft recommendation on the protection of medical data, working group 12)

However, recommendations have no legally binding force.

- European Community directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data (adopted by Council on 24 July 1995)
- National legislation related to the protection of personal data.

At the present time most of the Member States (except Italy) have adopted data protection legislation. Member States with existing national data protection will need to modify it in order to comply with the EC directive. Member States without data protection legislation will need to adopt legislation in conformity with the directive.

We will therefore examine the EC directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data in order to examine whether the principles laid down in the directive provide adequate protection of personal data in the use of health telematics.

THE EC DATA PROTECTION DIRECTIVE

In order to remove the obstacles to the free flow of personal data on data protection grounds caused by the divergence between the existing national legislation, the EC directive aims at coordinating the laws of the different Member States so as to ensure an 'equivalent' level of protection throughout the European Union. Member States will no longer be able to restrict nor prohibit the free movement of data between them on grounds relating to the protection of rights and freedoms of individuals, in particular the right to privacy **(Article 1** of the directive).

Because we cannot examine all the different national data protection legislation, we consider the EC directive as a common denominator. Our main purpose is to underline some of the issues raised when applying the requirements of the directive to a health telematics project.

I. DOES THE DIRECTIVE APPLY TO HEALTH TELEMATICS PROJECTS?

First and foremost one must enquire as to whether the directive applies to a health telematics project. According to **Article 3.1**. the "directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system".

1. PROCESSING OF PERSONAL DATA:

The processing of personal data is defined by the directive as:

> "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as the collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction" **(Article 2b).**

To the extent that the use of telematics in the healthcare sector involves the collecting, transmitting, processing and storing of personal data, the directive will apply.

Processing of personal data may take place at different moments, by different users and for different purposes. One

will need to identify when one can consider that personal data is being 'processed'. Processing can imply one operation in itself or sets of operations. We believe that in order to differentiate between the different processing, one must look at the purpose of the operations. The change of purpose (or finality) in the processing of the data implies a new processing. The existence of processing of personal data is identified by its purpose. This criteria enables us to adequately apply the principles laid down by the directive (such as legitimate purpose, conformity of data,...) as shown by the following examples: in a central network containing computerized medical records (a hospital X for example), the hospital processes the data so as to make it available to the different users of the service (processing of personal data in order to provide services to the users). A general practitioner located in hospital X may in turn consult a record so as to afford adequate care to the patient concerned. He may, if authorized to do so, introduce new data so as to update the record following the patient's visit (processing of the data so as to afford continuity of care). The medical data in a record may be further processed by a specialist in his private surgery when he is consulted a few weeks later by the same patient for further medical treatment (processing of the data by the specialist in order to afford care).

A patient data card (chipcard containing data relating to a patient) is a data bank in itself and can therefore be considered as a processing of personal data according to the directive. The card can also be considered at the heart of different processing of personal data by different players who either retrieve information from the card or introduce new data into the card. Hence the data card must be envisaged not only as a processing in itself but also at the centre of different processing operated by the different players involved in a patient data card system (physicians who consult the card to retrieve his patient's medical record in order to afford adequate care and who may (if authorized to do so) introduce data into the record so as to update the record following the patient's visit; social security institutions who may consult the card for patient reimbursement; pharmacists who may consult the card so as to provide the adequate medication; ...)

See *Figure 1*.

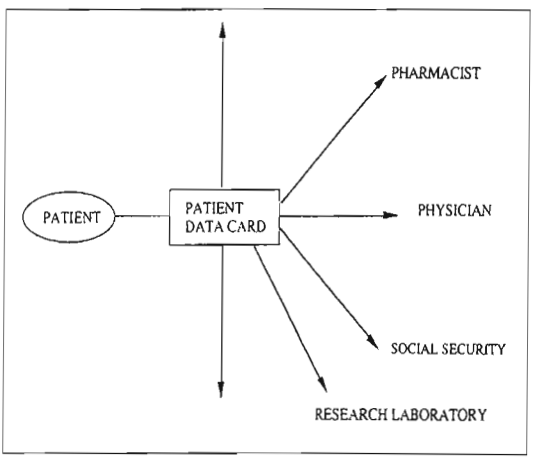

Figure 1. Patient data card a centralized data bank.

2. PERSONAL DATA: "INFORMATION RELATING TO AN IDENTIFIED OR IDENTIFIABLE NATURAL PERSON" (Article 2A)

"Information" can be written data, but also images, sounds... in so much as they relate to an identified or identifiable person. "Identified or identifiable natural person ": The data may relate to an identified person or to an identifiable person. It is noticeable that data relative to a dead person can still be considered as nominative data. The French law dated 1 July 1994 about medical research asserts that a person can refuse the use of his data after his death (art. 40.4. loi no. 94.548, J.O., 2 juillet 1995, p. 9559) To determine whether a person is identifiable all the means likely reasonably to be used to identify the said person must be taken into account. Coded data can be defined as personal data if one has the means to decode it. The identification of an individual may sometimes result in an aggregate of data: data when taken on its own may not always enable the identification of the patient, but does so when combined with other data (for example: an image may not enable identification of an individual but will do so if combined with the patient's illness, localization etc.).

Two types of data can be identified in the use of telematic services:

- "Patient related data": any data, whether medical or not, which concerns an identified or identifiable patient. Data concerning an individual's health is considered as a special category of data by the directive and appropriate safeguards are enacted so as to ensure a maximal protection (see later **Article 8**).
- "User related data": any data relating to the user.

For security or liability issues, the use of telematics in the healthcare sector can imply that the user identifies himself before using the service. Thus personal data concerning the said user is introduced into the network by the user himself. The use of telematics can also create a set of data concerning the user. For example, every time an identified or identifiable general practitioner exchanges medical information over a network, he reveals data concerning himself which can be used by the service or network provider not only so as to claim payment for the service used but also, for example, to monitor the user's activities or create user personal profiles.

II. DETERMINE WHO IS THE CONTROLLER (ARTICLE 2D)

"The controller is the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data."

It is important to determine who is the controller because he is responsible for fulfilling the obligations laid down in the directive and ensuring that the data subjects' (in this case the patients') rights are respected. The determination of the controller also determines the national law applicable to the project.

Article 4 of the directive states that each Member State shall apply the national provisions it adopts pursuant to this directive to the processing of personal data where the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; where

the same controller is established on the territory of several Member States, he will have to ensure that each of the establishments respect the national law of each of these States. (By "establishment" the directive means the effective and real exercise of activity through stable arrangements). A controller not established on the territory of the Community, will need to respect the member State's national law if he makes use, for the purposes of processing personal data on equipment, automated or otherwise, situated within the territory of that Member State. This will not, however, be the case if he only uses the equipment for purposes of transit through the territory of the Community. This is to avoid a controller circumventing the application of national law by locating himself outside the Community territory. In this event, he will need to designate a representative situated in the territory of that Member State.

The idea of one unique controller responsible for the processing of the data is commendable because it facilitates the respect of the principles laid down in the directive by one unique person and it enables the data subject to exercise his rights effectively. However, because the use of telematics in the healthcare sector very often implies a decentralization of the different operations applied on the personal data, it is not always easy to determine who is the controller amongst the different actors involved in a project. Matters are further complicated when providers of the network services are introduced (providing telecommunication services, providing EDI facilities...).

The use of telematics in the healthcare sector involves a certain number of players:

The telematics service provider: The person (legal or natural) or institution who offers the telematic services to the different users. For example provides telemedecine services, provides information services for citizens and healthcare workers, centralizes multimedia medical records so as to enable them to be communicated and combined, ...

The service users: The persons (legal or natural) or institutions who make use of the service provided (hospitals, insurance companies, social-security institutions, clinical labs, general practitioners, nurses, therapists, healthcare authorities and managers...).

The network provider: The entity which provides the communication infrastructure (telecommunication network, ISDN...) necessary to enable the flow of the information between the different users or between the users and the service providers. The telematics service provider and the network provider may be the same entity.

Trusted third parties: Additional services (certification services or evidence related services ...) may also be provided by trusted third parties.

It is probably correct to say that there can be various 'controllers' involved in a telematics project:

- The telematics service provider is the controller of the global network. He defines the purposes (facilitate the communication between healthcare professionals, provide online information...) and means (whether these be technical or managerial) of the project in its entirety.
- In as much as the users of the project make use of personal data provided for by the network and process it for their own purposes they can be considered as controllers of this processing. For example, if a general practitioner integrates the data provided on a network in order to update his own medical records.
- *Network providers* (telecommunication network providers in telemedecine and new telematics services, for example) or trusted third parties will usually not have access to the data relating to the patient. Furthermore and principally, they do not define the purposes of the project. They merely provide the means for processing or transporting the data. It would be absurd to define them as controllers because they do not effectively process the personal data in itself but only as part of a message which they are transporting or processing. They can be considered as a 'processor', that is to say a natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the person which processes personal data on behalf of the controller.

In certain cases the network providers may process user-related data, for example to control the identification of the user or to bill the service rendered to the network user (if the payment of the service is not centralized by the global network service provider). In this respect they will be considered as 'controllers' of these specific functions.

III. RESPECT THE PRINCIPLES LAID DOWN IN THE DIRECTIVE

1. THE LEGITIMATE PURPOSE PRINCIPLE: THE DATA MUST BE COLLECTED FOR LEGITIMATE PURPOSES AND NOT FURTHER PROCESSED IN A WAY INCOMPATIBLE WITH THE PURPOSES FOR WHICH THEY WERE COLLECTED (ARTICLE 6 & 7).

This principle is the cornerstone of the protection afforded to the data subject by the directive. Very often it is not the data in itself which represents a risk for the individual but the use one makes of this data.

The processing of medical data in a healthcare telematics programme can serve various purposes: patient care delivery (i.e. serve as a communication tool, support diagnostic work, assess and manage risk for individual patients..); billing and reimbursement (i.e. process bills for services, submit insurance claims ...); scientific or research purposes . . .

Personal data may only be collected and processed for a legitimate purpose.

The legitimate grounds for which personal data can be processed are laid down in **Article 7** of the directive: personal data may only be processed either if the data subject has given his unambiguous consent, or if the processing is necessary for performance of a contract; or if the processing is necessary to comply with a legal obligation to which the controller is subject; or if the processing is necessary in order to protect vital interests of the data subject; or if the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or finally if the processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party or parties to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject.

Therefore, only processing based on one of these criteria may be considered as "legitimate" in the eyes of the directive (the scope left to the national supervisory authorities, for example, to determine the legitimacy of the purpose once these criteria have been respected is not clear).
Personal data "must not be further processed in a way incompatible with the purposes for which they were collected". Once the data has been collected secondary uses of data are facilitated in telematics projects because of the possibility of interconnecting different medical telematic systems increasing the possibility of producing a very complete profile of any patient. It is important that the data collected for a specific and legitimate purpose is not reused in a different context considered as "incompatible". Individuals must have a means of preventing information, obtained from them for one purpose, from being used or being made available for other purposes. If in some cases the incompatibility of the purposes are evident (for example data collected when telemonitoring a person at home must not be used in order to control a persons' personal activities). In other cases the intervention of a national supervisory authority (see **Article 28** of directive) will be required to assess the "compatibility" of the secondary use with the purpose for which the data was initially collected.
Article 6.1.b. specifically states that "further processing for historical, statistical or scientific purposes shall not be considered as incompatible providing that the Member states provide appropriate safeguards". The transmission to and processing of medical data by research laboratories is therefore not considered as incompatible. Adequate safeguards could include the encryption of the data whilst being transmitted through the network.

2. THE PROHIBITION UNDERLYING THE PROCESSING OF SENSITIVE DATA (ARTICLE 8)

The processing of sensitive data is prohibited according to Article 8.1 of the directive. Some exemptions to this prohibition are however stated in the directive **(Article 8)**.
Data concerning an individual's health is considered by the directive as sensitive data. Therefore any healthcare telematic project which processes personal medical data must find grounds in article 8 enabling them to process the data.
What are the grounds which could lift the prohibition of processing of sensitive personal data?

(i) Data subject's consent

Article 8.2.a: Unless Member states decide that the data subject's consent cannot lift the prohibition to process sensitive data, the controller will need to obtain the explicit consent of the data subject prior to the processing of his data.
The health telematics project controller will therefore need to obtain the data subject's consent in order to process his personal medical data.
The EC directive defines data subject's consent as:
"any freely given specific informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed" **(Article 2.d)**.
A specific consent means consent for one well defined project or application. The data subject will not need to give his consent each time his data is processed, for every operation (for example, use of a blood sample for different tests). However one must avoid the use of blanket consent for generic finalities which are so vague that they do not enable an effective control of the uses of the data. The consent will need to be obtained for each new purpose, which is not compatible with the purpose for which the consent was originally given.
The data subject's consent may be obtained by the patient entering a personal code or handing over a chipcard enabling the professional to access his data.
Informed consent means that the patient has been adequately informed of the technologies used, of the controller, of the purposes of the processing etc. (see right of information). It must be reconciled with the limited right of access and of information as stated in **Article 13** (see limitations to right of information and right of access).
The consent must be freely given. This implies that no pressure is put on the patient, and that he will not be discriminated against if he does not give his consent. In health-related projects there is always an underlying fear that if the data subject does not give his consent he will not be entitled to the care he deserves.
Because the use of telematics introduces the concept of networks and the covering of wide distances between the healthcare professionals providing the services and the patients, the problem of how to obtain the data subject's consent may arise. The controller may not always be in the best position to obtain the data subject's consent: for example the telematics service provider may not be in direct contact with the patient.

(ii) Medical or health-related purposes and persons covered by professional secrecy or an equivalent obligation

Article 8.3. states that the prohibition to process sensitive data shall not apply where the processing of the data is required for purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of healthcare services, and where those data are processed by a health professional subject to national law or rules established by national competent bodies to the obligation of professional secrecy, or by another person also subject to an equivalent obligation of secrecy.
This provision could justify the processing of medical data in projects serving health related purposes (exchanging information between practitioners, the use of technical instruments, of knowledge-based decision systems, image processing...) between users covered by professional secrecy (or an equivalent obligation). This exemption is based on the idea that a balance must be struck between the legitimate right of the data subject to control the uses of his data by giving his express consent and the needs of the healthcare system to be able to process medical data without the burden of obtaining the data subject's consent. In most of the Member states the provision of medical care is subject to the data subject's consent (which may be implicit by the fact that the patient goes to see a healthcare professional for care). Thus one could say that the subject's consent to the treatment in itself implies the consent to the processing of personal data surrounding the provision of the care. As long as the persons processing the data are covered by professional secrecy or an equivalent obligation, the data will be able to be processed, regardless of the data

subject's consent. This exemption, in our view is limited to processing of personal data in a health-related context (hospitals, clinics,...). It enables the exchanges and use of a person's medical data by healthcare professionals (or persons covered by an equivalent obligation) without the consent of the data subject. The processing of personal medical data by a physician for insurance claims or employment purposes therefore falls outside the scope of this provision. This is especially true in countries in which the physician is not subject to professional secrecy with regard to the insurer or employer he works for.

The conditions and scope of persons covered by professional secrecy and the conditions in which they may reveal information amongst themselves for the purposes of a patient's treatment will need to be adequately defined. This is especially valid in the healthcare sector where the use of telematics extends the exchange of medical information and data between healthcare professionals beyond the scope of the medical team or institution. The exact scope of this exception will therefore very much depend on national legislative or professional rules governing professional secrecy

(iii) To protect the vital interests of the data subject

Article 8.2.c: Processing of sensitive data is allowed if necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent.

This provision enables the processing of sensitive data even if the data subject is physically or mentally incapable of giving his consent. Distance however is not, in our opinion, a sufficiently good reason to justify the use of this provision.

The processing of medical data in vital emergency situations (when a patient is in an *'in extremis'* situation and is not in a position to give his consent, for example) could be permitted under this provision. One will however need to determine what are the "vital interests of the data subject or of another person" and ensure that the processing was indeed necessary to defend this interest. This provision could justify the processing of personal data in order to save a patient's life. Only that data necessary to protect the vital interests may be processed (see conformity principle).

(iV) Further exemptions provided for by the member states

Article 8.4: Member States may "subject to the provision of suitable safeguards, for reasons of substantial public interest, lay down exemptions in addition to those laid down in paragraph 2 either by national law or by decision of the supervisory authority".

Some projects may therefore be based on these measures adopted by the Member States.

3. DATA QUALITY (ARTICLE 6)

Certain data quality requirements are laid down in the directive. It is up to the controller to ensure that these are respected.

(i) Personal data must be "processed fairly and lawfully" (Article 6.1.a)

Lawful processing implies that the principles laid down in chapter II of the directive are respected (principles relating to data quality, information to be given to data subject, respect of data subject's rights, confidentiality and security, and notification to the national public authorities).

Fair processing requires transparency. The patient's personal information must not be processed for any hidden or occult purposes. The patient concerned will be made aware of the uses of data relating to him either when the data is collected or when first recorded or first disclosed (see information to be given to the data subject). Any change of purpose in the processing of the data which is not compatible with the initial purpose must be revealed.

(ii) Personal data must be "collected for specified, explicit and legitimate purposes" (Article 6.1.b)

The legitimate grounds for which the processing of medical data is permitted were examined above. These purposes must be clearly defined and stated. It is only if the aims are clearly announced that the competent authorities and the data subject will be able effectively to control the uses of the data and the respect of the principles laid down in the directive.

(iii) The personal data must be "adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed" (Article 6.1.c.)

One must always ask oneself, what is the purpose of the processing? Is the data collected and recorded relevant and necessary for this purpose? The users should only have access to the data strictly necessary for the purposes of their processing. This provision may require the implementation of special security measures such as 'user-specific menus' to control access to functions and thereby limit user access only to particular parts of the patient record that the user legitimately needs to carry out his job. For example, an administrator may have the ability to view only accounting and demographic data but may have no access to medical data. The users may only exchange between themselves what is strictly necessary for their function.

For example, in an emergency situation telematics application, only the data considered as vital will be able to be accessed. This criterion will therefore be needed to determine the minimal, necessary data in an emergency situation.

(iv) The data must be "accurate and where necessary kept up to date" (Article 6.1.d)

It is not always easy to define data relating to a person's health as "accurate". If one can describe objective facts (images, clinical results,...) as accurate, it is difficult to describe subjective information such as a general practitioner's objective appreciation as accurate.

Computerization very often implies standardization of information so as to facilitate the gathering, exchanging and transmitting of data. If the network acquires an international dimension, the content of patient medical records will need to be standardized, this may imply that a nomenclature of medical data is established. Accurate data implies the use of the correct term of the nomenclature.

Accurate data also implies 'complete' data. Computerization on an international scale may imply the definition of minimum data sets to be required in each medical record. The completeness of a patient's record for subsequent users will

therefore depend in part, on agreements about uniform data elements.
Multimedia clinical records, for example, will need to be updated regularly: it is not easy to decide who will be responsible for updating the records. Compliance could result in the fact that each and every user is held responsible for updating the data he has access to.

(v) " Every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or which they are further processed, are erased or rectified " .
It is up to each controller to ensure that the principles concerning the data quality are respected concerning his processing of the data and that inaccurate or incomplete data are erased or rectified. Because the telematics service provider is not always in the best position to ensure the quality of the data, he may choose to ensure that the data is controlled in this respect by each user each time he consults the information.

(vi) Personal data may only be "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data are collected or for which they are further processed" (Article 6.1.e).
The data storage should be regularly reviewed so as to ensure that only the necessary data for the purposes of the service offered is conserved. Thus the global telematics service provider may only store data relating to patients for as long as this data is necessary to afford the patient with adequate medical treatment. The network provider (telecommunications network provider, for example) should not, in principle, conserve the data which has been transmitted through the network and concerning an individual patient (except if he has been appointed with evidence related responsibilities). The telecommunications service provider may however conserve data relating to the user of the service for billing purposes (unless the billing of the services is centralized by the telematics service provider).

4. THE DATA SUBJECTS' RIGHTS

The EC directive creates rights for the data subject. The controller (or his representative) will need to ensure that these rights are provided for.

(i) Right to be informed (Articles 10 and 11)

When the data is collected from the data subject he will need to be informed at least with the following information, except when he already has it:

- the identity of the controller or of his representative
- the purposes of the processing for which the data are intended
- and any further information such as: the recipients or categories of recipients of the data; whether replies to questions are obligatory or voluntary, as well as the possible consequences of a failure to reply; the existence of a right of access to and right to rectify the data concerning him in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.

When the data has not been obtained from the data subject (e.g. transmission of medical data from a general practitioner to a clinical lab for analysis via a communications network), the data subject will need to be informed of the information stated above, at least when the data is recorded or, in the event that the data are disclosed to a third party, at the time of the disclosure.
The data subject has a right to be informed. If the processing of the sensitive data is based on the data subject's consent, adequate information of the subject is a fundamental element of this consent. Appropriate measures will therefore need to be taken to ensure that the data subject is properly informed. Initial information of the data subject will need to be sufficiently wide so as to ensure that the subject is aware of the uses of the data relating to him. (However, one will need to avoid the use of generic definitions which do not permit the effective surveillance as to the uses of the data by the controller.)
When the data has not been collected from the data subject it is very often the case that the person processing the data has no direct contact with the individual. How will he be able to ensure the adequate information is effectively given? It could be a good idea to designate a person held responsible for informing the data subject. Information could be given in brochures, on posters...
Limitations of the right to be informed (article 13):
The EC directive provides that the Member States may adopt legislative measures to restrict the scope of the right to be informed, for example if such a restriction constitutes a measure necessary to safeguard: "the protection of the data subject or the rights and freedoms of others".
A Member State may therefore judge that the data subject need not be informed of the identification of the recipients or categories of recipients to whom the data is disclosed (a cancer research laboratory for example.) if this could be detrimental to his health. In the event of apprehensions of the patient concerning his medical condition, the health professional's silence may be badly interpreted.

(ii) Data subject's right of access to data (article 12)

The data subject is given:

> "the right to obtain from the controller, without constraint at reasonable intervals and without delay or excessive expense, confirmation that data relating to him are being processed, and information at least as to the purposes of the processing, the categories of data concerned and the recipients or categories of recipients to whom the data are disclosed; communication in an intelligible form of the data undergoing processing and information available as to their source, knowledge of the logic involved in any automatic processing of data concerning him at least in the case of automated decisions".

The controller of the telematics network will therefore need to ensure that this right of access to the data contained in telematics applications can be effectively exercised. He may need to set up technical means whereby this right can be put into effect (online access to the data by the patient, setting up of a 'bureau' to whom the data subject can address himself for

access to his data...). He may need to delegate this obligation to the users of the network if he is not in direct contact with the individual concerned (one could imagine for example that in the case of computerized medical records centralised by a service provider, the access of the patient to his record is afforded by the patient's general practitioner) .

LIMITATIONS TO THE RIGHT OF ACCESS (ARTICLE 13 G):
Member States may limit this right if this restriction is "necessary to protect the rights and freedoms of the data subject or of others". The directive specifies that, for example, the right of access to medical data may only be obtained through a health professional. This provision enables the right of access to be reconciled with the concept of medical secrecy existing in some of the Member States, restricting the patient's access to his medical record when this access could prove detrimental to his condition. This restriction is not, however, to be found in every Member State. In projects ranging over several Member States, the extent of the access to the personal data transmitted on a network may therefore vary from country to country. Furthermore one may question the competence of the healthcare professional to "filter" the data which he affords to the patient: may he, in the interests of the patient, limit the information which he gives to the patient and regarding his medical condition? Access to one's personal data can reveal information about another person. This is so in the case of certain genetic information, for example, which reveals medical information about persons belonging to the same genetic line. In order to protect the rights of another person, one could also envisage a limitation on the right of access. A balance will need to be struck between the data subject's right of access and the right to privacy of the other person.

(iii) The right of rectification
The right of access is set up so that the data subject can challenge the accuracy of the data and the lawfulness of the processing. The data subject is afforded with a right of rectification, erasure or blocking of data, in particular because of the inaccurate or incomplete nature of the data.
Limits to the right of access and right of rectification Article 13g):
Member States are allowed to restrict this right if this restriction is necessary to safeguard the data subject. This provision could prove useful. It is sometimes difficult to speak of "accurate medical data" (see. *supra*). Furthermore, the blocking of certain data may prove detrimental to the person's health if the fact can later be useful for a medical treatment.

(iv) The data subject's right to object (Article 14 a)
Member States shall grant the data subject with the right "to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided for by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data".
The right to object applies to certain data and not to the processing in itself. The subject will therefore be able to block the use of certain data but will not be able to oppose the processing in itself. He will, however, need to base his right on compelling legitimate grounds. In projects with a health related purpose, it is unlikely that he will be able to exercise his right in so far as it could lead to detrimental effects for him.

(v) Automated individual decisions (article 15.1)
"Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc."
This provision aims at preventing decisions taken solely on the basis of an automatic processing of data. It aims at reintroducing the intervention of an individual in order to assess the situation and adopt an adequate decision. It could apply in the case of software tools used for automatic processing of multimedia data sets, images, clinical graphs and drawings etc. e.g. for taking a decision concerning a patient's medical treatment for example.

(vi) The Controller's obligations
- Obligation to inform the data subject **(Articles 10 and 11)**
  The controller must provide the data subject with a certain amount of information so as to ensure a maximum of transparency in the processing of his data. This obligation corresponds to the data subject's right to be informed.
- Notification of the processing **(Article 18)**
  The controller or his representative must notify the supervisory authority before carrying out any wholly or partly automatic processing operation or set of such operations intended to serve a single purpose or several related purposes.
  The object of this provision is to ensure disclosure of the purpose and main features of any processing operation for the purpose of ensuring that the operation or set of operations respect the national measures.
- Security of processing **(Article 17)**
  "The controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.
  Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected."

The introduction of networks increases the risks involved in the processing of the data. The risks incurred are notably the threat of access to the data by unauthorized persons and the unauthorized use of the data by authorized users.
For example, computerization implies standardization of medical information in both content and format. Content standardization, for example, enables secondary users to anticipate the nature of the information and its uses.
Furthermore computerization and networks implies the possibility of linkages. (By linkages we mean the possibility of interconnecting different computer systems enabling them to interact effectively.) It will be easier to break into an electronic data bank and retrieve unlimited information. The use of a unique patient identifier, for example, has the advantage of assigning the patient with an identifier from birth to death, to

ensure appropriate, accurate information exchange among the approved parties, prevent fraud in reimbursement and ensure accurate linkage of information between different users. However, it also increases the risks involved due to the power of the identifier to act as a key to uncovering and linking a vast amount of information in order to create a very complete personal profile.

It must be recognized, however, that even though the use of telematics increases the risks for a patient's privacy and the confidentiality of the information, computer-based systems may be even more secure than paper-based systems. Telematics may serve as an instrument in order to protect the data (see later: use of an access card, introduction of a PIN code, etc. in order to control access to data; authentication, electronic signature, audit trails etc. in order to control circulation of information ...).

The *nature of the data* being of a particularly sensitive nature, and the risks in health telematics projects being acute, the controllers of a health telematics project will need to afford a high level of protection. However, the health sector is unique in that information must be able to circulate freely and quickly amongst authorized users. A patient's life may depend on a certain person being able to access the necessary data in a number of minutes. It is recommended therefore to maintain a balanced approach between security and privacy so as to avoid handicapping the development of systems through the abuse of security requirements.

The *security measures* adopted can be of a technical or of an organizational nature. They can be afforded at different levels: access controls through the use of PIN codes, user identification, or access cards; authentication of the data; protection during the transmission of the data by encryption of the data, coding of the data, audit trails...

The directive mentions some of the organizational measures to be taken. For example, it stipulates that the "Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures". The controller will therefore need to determine the community of authorized users.

IV TRANSBORDER DATA FLOWS

DATA FLOWS WITHIN THE EU

The directive aims at ensuring an equivalent level of protection throughout the Union, therefore, Member States will no longer be able to prohibit the free flow of personal data between them for reasons related to data protection. European Union-wide telematic programs will therefore be facilitated, even though, despite harmonization of national legislation, differences will continue to subsist. (This is a result of the "margin for manoeuvre" which the directive affords to the Member States). These differences could raise some practical problems. For example, the Member States may grant the data subject different levels of access to their personal data flows outside the EC (**Article 25** and following).

A telematic project which intends to transfer personal information to a third country may only do so if the third country in question ensures an "adequate level of protection". Special rules for evaluating the "adequate" level of the protection are developed in the directive. We will refrain from going into these.

V CODES OF CONDUCT (ARTICLE 27)

The EC directive encourages the drawing up of codes of conduct intended to contribute to the proper implementation of the national provisions adopted by the Member States pursuant to the directive. In view of some of the specific issues raised by the use of technologies in the health care sector, sector-based codes of conduct could provide a more flexible and adequate approach.

One must not undermine the role of professional associations in the setting up of computerized networks in the healthcare sector: in providing information about the flows of information between healthcare professionals, in standardizing medical data, in authorizing the users, in the determination of the access to the data and determination of the operations permitted by each type of healthcare professional.

CONCLUSION

The EC directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data goes beyond the protection afforded by the traditional secrecy in a certain number of ways.

The directive permits the exchange of personal medical data between a wider group of authorized users, providing they respect the finality principle. It therefore extends the possibilities of sharing medical data beyond the institutional framework of the healthcare professional to other institutions or to research laboratories, for example. The principles laid down in the directive introduce effective control over who is entitled to process the data and on what grounds, to whom may he transmit the data, how long may he conserve the data ...

A justified apprehension regarding the use of telematics in the healthcare sector is the lack of transparency in the network. This is due in part to the multiple players involved in the network and the different roles they play in the processing of the information. The directive implies a greater responsibility on the part of the different players involved in a telematics application project, in so far as they are considered as 'controllers' and are therefore liable to the respect of a number of rights and obligations.

The objection to the lack of transparency of a telematics project is also reduced by the rights which the directive creates in regard to the data subject (right to be informed, right of access,...). these rights enable the data subject to maintain control over the use and transmission of his personal data.

Sophie Louveaux and **Yves Poullet**
Centre de Recherches Informatique et Droit, Rempart de al Vierge 5, B-5000 Namur, France.

FOOTNOTE
[1]The European legal framework for data protection and privacy. Study done in the context of the LEGASSIST research contract (DG XIII-F).